УДК 681.322 Вестник УрФО № 1(27) / 2018, с. 24–28

Баранкова И. И., Михайлова У. В., Лукьянов Г. И.

ПОДХОД К ПРОЕКТИРОВАНИЮ СЕТИ ПРЕДПРИЯТИЯ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

В современном информационном обществе ни одно предприятие или компания не может обойтись без создания собственной корпоративной сети. Такая сеть может быть выполнена как в пределах одного объекта или здания, но чаще применение находят сети с географическим распределением использующие сеть интернет. Передача информации в цифровом виде по сети значительно упрощает доступ злоумышленнику. Кража, изменение и другие действия над информацией злоумшлиником могут нанести значительный ущерб предприятию. В связи с этим безопасность вычислительных корпоративных сетей является важной составляющей современных информационных технологий компьютерной безопасности для любого предприятия. В данной статье рассмотрено проектирование защищенной корпоративной сети предприятия, которое обеспечивает компьютерам данной сети выход в интернет. Разработанная сеть позволяет взаимодействовать филиалам между собой, а так же использовать кроме проводной связи и беспроводную. В спроектированной корпоративной сети обеспечена скорость доступа к интернету на высоком уровне за счет использования высокоскоростных каналов доступа и распределения нагрузки между устройствами. Безопасность спроектированной сети осуществляется за счет применения технологии VLAN, а так же за счет использования списков доступа и AAA-сервера. В зависимости от типа информации и требуемого уровня защиты возможно повышение устойчивости корпоративной сети к атакам из внутренней и внешней сети за счет программных и программно-аппаратных средств защиты информации.

Ключевые слова: *корпоративные сети, безопасность сетей, утечка информации, сетевые атаки, проектирование сетей, каналы доступа, списки доступа, AAA-сервер, VLAN, LAN, ARP-запросы, Ethernet.*

Barankova I. I., Mikhailova U. V., Lukianov G. I.

APPROACH TO THE DESIGN OF THE ENTERPRISE NETWORK IN A PROTECTED DESIGN

In today's information society, no enterprise or company can do without creating its own corporate network. Such a network can be performed as within a single object or building, but more often the use of networks with geographical distribution using the Internet. The transmission of information digitally over the network greatly simplifies access to the attacker. Theft, alteration and other actions on the information by the evil-doer can cause significant damage to the company. In this regard, the security of computing corporate networks is an important

component of modern information technologies of computer security for any enterprise. This article discusses the design of a secure corporate network of the enterprise, which provides computers of the network access to the Internet. The developed network allows branches to interact with each other, as well as use except wired and wireless communication. Designed in the corporate network, provided the speed of Internet access at a high level through the use of high-speed access channels and load balancing between devices. The security of the designed network is carried out through the use of VLAN technology, as well as through the use of access lists and AAA-server. Depending on the type of information and the level of protection required, it is possible to increase the resistance of the corporate network to attacks from the internal and external networks through software and hardware-software information security.

Keywords: *corporate networks, security of networks, information leakage, network attack, network design, access channels, access lists, AAA server, VLAN, LAN, ARPS, Ethernet.*

В современном информационном обществе ни одно предприятие и компания не может обойтись без создания собственной корпоративной сети. Это ускоряет и облегчает работу сотрудников на любом уровне. Но содержит большую угрозу для конфиденциальной информации предприятия. Универсальным средством защиты сети до недавнего времени от нежелательного трафика был межсетевой экран. В настоящее время абсолютную безопасность не может гарантировать ни одна из применяемых технологий [1; 2]. Сетевые атаки становятся год от года все более изощренными, все более активным становится использование методов социальной инженерии. Обеспечение безопасности вычислительных сетей это трудоемкий и сложный процесс, заключающийся в разработке и проведении целого комплекса организационных и технических мероприятий, направленных на достижение следующих целей:

1. Существенное затруднение для злоумышленника возможности произвести сбор информации об интересующей его вычислительной сети [3].

2. Минимизация возможностей для проникновения злоумышленника внутрь охраняемого периметра защищаемой организации и подключения его к локальной вычислительной сети организации [4].

3. Исключение ситуаций возможности перехвата сетевого трафика злоумышленником, если его попытка подключения к локальной вычислительной сети «жертвы» все-таки увенчалась успехом [5].

Первое что необходимо выполнить для обеспечения безопасности проектируемой сети это ее структурирование. Для этого необходимо изучить масштаб предприятия. В данной статье локальная сеть предприятия в защищенном исполнении проектируется для предприятия, в котором имеется два пятиэтажных здания, в каждом из которых находится по семь рабочих групп, по десять рабочих станций в каждой. В процессе проектирования сети предприятия спланирована структура вычислительной сети. Первоначально сегментируется вычислительная сеть, затем определяется схема адресации и осуществляется выбор схемы управления обменом сетевым трафиком между VLAN. Проектирование выполняли в пакете«Ciscopackettracer». Размещение ПК и подключения их к сетевому оборудованию приведены на рис. 1.

Трафик, передаваемый в пределах локальной вычислительной сети, может быть как широковещательным, так и предназначенным конкретному абоненту. При подключении нового компьютера к вычислительной сети Ethernet данный компьютер начинает опрос других компьютеров сети при помощи протокола ARP, рассылая им широковещательные ARP-запросы. Получив от них ответы, компьютер добавляет их MAC-адреса в свою ARP-таблицу. Количество сетевого трафика по протоколу ARP будет превышать все прочие виды трафика, что создаст непроизводительную нагрузку на сетевую инфраструктуру. Более того, обладание информацией обо всех абонентах сети для рядового компьютера в сети является совершенно избыточным. Так же обладание информацией обо всех устройствах сети несет угрозу сетевой безопасности, ибо полномочия сетевых узлов и их пользователей, а также важность обрабатываемой ими информацией и ее характер, могут существенно различаться.

Для устранения вышеперечисленных недостатков сети используем технологии создания виртуальных локальных вычислительных сетей (VLAN). VLAN имеет те же свойства, что и физическая локальная сеть, но позволяет конечным станциям группироваться вместе, даже если они не находятся в одной физической сети. Такая реорганизация может быть сделана на ос-

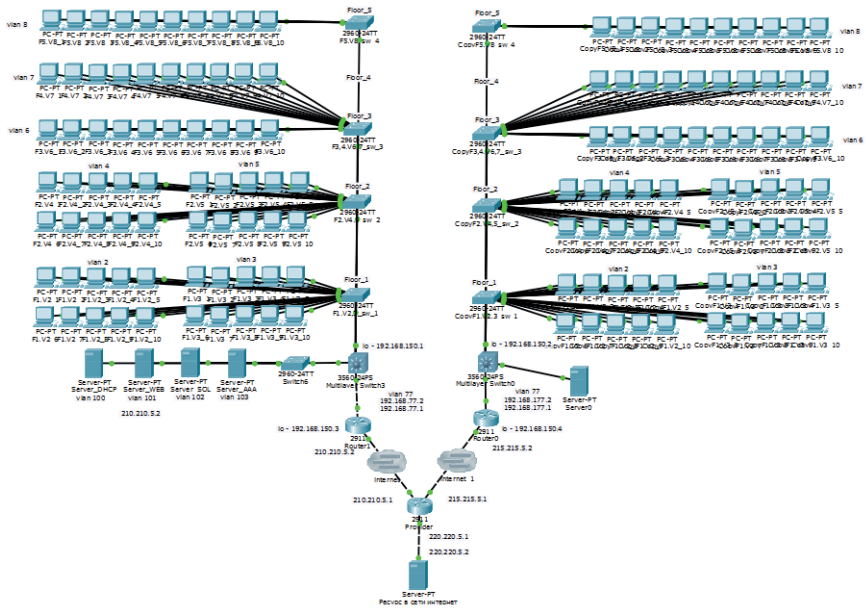

Рис. 1. Схема размещения ПК предприятия и подключения их к сетевому оборудованию

нове программного обеспечения вместо физического перемещения устройств. Согласно данному стандарту, виртуальная ЛВС организуется следующим образом:

1. На сетевых устройствах объявляется виртуальная ЛВС путем задания специальной метки – тэга. Данная метка присваивается сетевым портам коммутаторов ЛВС, к которым подключены группируемые в виртуальную ЛВС сетевые узлы.

2. Сетевой трафик, исходящий от устройств, подключенных к помеченным таким образом портам, маркируется путем присоединения метки VLAN к заголовкам кадров Ethernet. Трафик, тем самым, становится помеченным.

Для этого выполнили настройку VLAN на оборудовании CISCO со всеми рабочими группами на всех коммутаторах второго уровня. Порты которыми коммутаторы второго уровня подключены к коммутаторам третьего уровня сделали trunk портами так как через них будет поступать трафик адресованный к разным устройствам. В результате получили конфигурацию, приведенную на рис. 2.

```
Switch#sho vl br

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/22, Fa0/23, Fa0/24, Gig0/1
                                                 Gig0/2
2    Flor_1_vl_2                       active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                 Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10, Fa0/11
3    Flor_1_vl_3                       active    Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                 Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                 Fa0/20, Fa0/21
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
Switch#
```

Рис. 2. Конфигурация настроек коммутатора второго уровня

Аналогичные настройки, но с другой нумерацией VLAN'ов проделаны на всех коммутаторах второго уровня.

Коммутатор третьего уровня в отличие от коммутаторов второго уровня осуществляет маршрутизацию трафика с помощью IP адресов. Для этого созданы VLAN'ы для каждой отдельной сети и каждому из них присвоены IP адреса из своей сети. Для динамической маршрутизации с использованием технологии OSPF создан интерфейс локальной петли и перечислены сети к которым существует доступ через этот коммутатор, сделано это для того чтобы не писать отдельно статические маршруты на каждом устройстве. Так же настроен статический маршрут из всех сетей на порт роутера, для выхода в Интернет. Получение IP адресов на ПК осуществляется с помощью выделенного DHCP-сервера. Роутер защитили с помощью пароля, а для дополнительной безопасности использован AAA-сервер. Сервер AAA используется для хранения учетных записей пользователей и дополнительно повышает безопасность и удобство администрирования сети, за счет централизованного управления учетными записями.

Заключение

Описанный в статье подход к проектированию ЛВС предприятия обеспечивает компьютерам данной сети выход в интернет, так же произведена настройка взаимодействия с филиалом, обеспечена скорость доступа к интернету на высоком уровне за счет использо-

вания высокоскоростных каналов доступа и распределения нагрузки между устройствами. Безопасность спроектированной сети осуществляется за счет применения технологии VLAN, а так же за счет использования списков доступа и AAA – сервера. Спроектированная описанным выше образом корпоративная сеть обеспечит оптимально безопасную передачу данных предприятия без использования дополнительных средств защиты информации. В случае необходимости усиленной защиты информации использование специальных средств защиты информации будет обязательным.

Литература

1. Barankova I., Mikhailova U., Lu'yanov G. Automated control system of a factory rail way transport based on ZIGBEE // 2016 2nd International Conference on Industrial Engineering, Applications and Manufacturing, ICIEAM – Proseedings. 2016.

2. Баранкова И.И., Михайлова У.В., Лукьянов Г.И. DLP система: защита от утечки информации. Анализ поиска WordSearch // Актуальные проблемы современной науки, техники и образования, 2016. Т. 1. № 1. С. 187-191.

3. Баранкова И.И., Михайлова У.В., Лукьянов Г.И. Прогнозирование локальных и внешних угроз на информационные серверы предприятия // Актуальные проблемы современной науки, техники и образования. – 2017. – Т. 1. С. 217-220.

4. Баранкова И.И., Михайлова У.В., Самохвал В.Д., Огонесян Ш.У Анализ информационных угроз вуза // Актуальные проблемы современной науки, техники и образования. – 2013. – Т. 2. – № 71. С. 157-159.

5. Коновалов М.В., Михайлова У.В., Хусаинов А.А., Санарбаев Р.Ж. Алгоритмы шифрования данных // Актуальные проблемы современной науки, техники и образования. – 2013. – Т. 2. – № 71. С. 159-161.

References

1. Barankova I., Mikhailova U., Lu'yanov G. Automated control system of a factory rail way transport based on ZIGBEE // 2016 2nd International Conference on Industrial Engineering, Applications and Manufacturing, ICIEAM – Proseedings. 2016.

2. Barankova I.I, Mikhailova U.V., Lukyanov G.I. DLP sistema: zashchita ot utechki informatsii. Analiz poiska WordSearch[DLP system: protection against information leakage. WordSearch search analysis] // Aktual'nye problemy sovremennoy nauki, tekhniki i obrazovaniya [Actual Problems of Modern Science, Technology and Education], 2016. T. 1. № 1. P. 187-191.

3. Barankova I.I, Mikhailova U.V., Lukyanov G.I. Prognozirovanie lokal'nykh i vneshnikh ugroz na informatsionnye servery predpriyatiya [Forecasting of local and external threats to enterprise information servers] // Aktual'nye problemy sovremennoy nauki, tekhniki i obrazovaniya [Actual Problems of Modern Science, Technology and Education], 2017. T. 1. P. 217-220.

4. Barankova I.I, Mikhailova U.V., Samohval V.D., Oganesyan Sh.U. Analiz informatsionnykh ugroz VUZA [Analysis of information threats of the University] // Aktual'nye problemy sovremennoy nauki, tekhniki i obrazovaniya [Actual Problems of Modern Science, Technology and Education], 2013. T. 2. № 71 P. 157-159.

5. Konovalov M.V., Mikhailova U.V., Husainov A.A., Sanarbaev R.J. Algoritmy shifrovaniya dannykh [Data Encryption Algorithms] // Aktual'nye problemy sovremennoy nauki, tekhniki i obrazovaniya [Actual Problems of Modern Science, Technology and Education], 2013. T. 2. № 71 P. 159-161.

Баранкова Инна Ильинична, доктор технических наук, заведующий кафедрой ИиИБ, Магнитогорский государственный технический университет им. Г. И. Носова. 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: inna_barankova@mail.ru

Михайлова Ульяна Владимировна, кандидат технических наук, доцент кафедры ИиИБ, Магнитогорский государственный технический университет им. Г. И. Носова. 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: ylianapost@gmail.com

Лукьянов Георгий Игоревич, ассистент кафедры ИиИБ Магнитогорский государственный технический университет им. Г. И. Носова 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: decorsi@mail.ru.

Barankova Inna, Department, Nosov Magnitogorsk State Technical University (NMSTU), D. Sc.,Head of Computer Science and Information Safety Engineering (CSISE), Bld. 38, Lenina Ave, Magnitogorsk, Russia, 455000, E-mail: inna_barankova@mail.ru;

Mikhailova Uliana, NMSTU, Ph.D.,Associate Professor of CSISE Department, Bld. 38, Lenina Ave,

Magnitogorsk, Russia, 455000, E-mail: ylianapost@gmail.com;

Lukianov Georgy, NMSTU, Teaching Assistant of CSISE Department, Bld. 38, Lenina Ave, Magnitogorsk, Russia, 455000, E-mail: decorsi@mail.ru.